POLICY 1335.00 Information Technology Access Control
Issued April 12, 2007

SUBJECT: Policy for Information Technology Access Control

APPLICATION: This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using State information networks and IT resources.

PURPOSE: This policy establishes the State of Michigan (SOM) executive management strategic view of how employees and trusted partners shall obtain access to established services on the SOM network. This policy further establishes the protection of information and systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users. Such access must be controlled with secure means of authentication, authorization and accountability.

This policy focus is on users obtaining access to established SOM services. If a service does not exist, the **SOM Network & Infrastructure Policy** will direct you to compliance in establishing a new SOM service.

CONTACT AGENCY: Michigan Department of Information Technology (MDIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: **Access Control** is the protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities.

Access to SOM network and IT resources and other technology resources shall be strictly controlled such that only SOM authorized users have access to the available information.

This policy will define the access controls required prior to users and systems gaining access to the SOM network and IT resources, controlling the actions they can take and track what action was taken on the resources the user has accessed. This policy is based on three basic components of access control and they are defined as:

Authentication is the process of determining whether someone or something (system) is, in fact, who or what it is declared to be. Example: use of a password to confirm correct association with a username or account name.

Authorization is the process of giving the authenticated person or system access to SOM network and IT resources and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.

Accountability is the process of determining the identity, activity and usage of a system by a user or system.

POLICY:

It is the Agency/Department who gathers data, enters it into the system, verifies its accuracy, specifies the purposes to which it can or will be used, designates who can use it, and ultimately, fills a business need through its use.

- Agency responsibility as Data Owners
  - Each Agency Director within their area of responsibility shall ensure:
    a. A formalized process is developed to manage user access to SOM Network and IT resources in compliance with this and all SOM policies that:
       aa. Limit access to authorized users whose job responsibilities require it as determined by the agency internal approval process.
       bb. Allow access to be managed, controlled and periodically reviewed and audited to ensure user access is based on specific privilege granted.
       cc. Provide a mechanism for controlling and documenting the allocation of user access rights from initial access rights, as a new user, through to de-registration, when the user change jobs or leaves the agency.
       dd. Utilize methods that provide user authentication, authorization and accountability.
       ee. Promote separation of duties, least privilege and a need to know.
       ff. Ensure users approved to access established services on the SOM network and IT resources are approved in compliance with this and all SOM policies.
    b. Internal agency security polices and procedures are implemented, maintained and enforced that compliment and comply with this policy.
    c. State Departments desiring to implement more stringent policies than those developed by MDIT may do so in conjunction with MDIT.

- Agency responsibility as Data Custodians:
  - The Department of Information Technology Director shall ensure:
    a. All agencies have access to the SOM policies, standards, procedures and guidelines governing user access to the SOM network and IT resources.
    b. A formal process is established to manage user access to the SOM network and IT resources (LAN, WAN, file and print, desktop, etc.).
    c. A formal process is established to implement and audit agency approved access requests to established services (i.e. wireless, Telecom catalog services, application access, new employee access, etc.) on the SOM network in compliance with this and all SOM policies.
    d. A formal process is established that ensures the proper implementation and integration of service continuity with other system operations and technical security controls as prescribed by MDIT in conjunction with the agencies.

Terms and Definitions

Agencies	Is the principal department of state government as created by Executive Organization Act 380 of 1965.
Availability	Ensuring timely and reliable access to and use of information and assuring that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.
Business Owner	Responsible for administration of systems is usually the owner of the primary business functions served by the application, the application's largest stakeholder.
Confidentiality	Protecting information from unauthorized disclosure or interception and assuring that information is shared only among authorized persons and organizations.
Data Custodian	The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of their data and systems.
Data/Information	Is SOM Agency information. No distinctions between the words data and information are made for purposes of this policy.
Data Owner	Usually a member of senior management of an organization and is ultimately responsible for ensuring the protection and use of the data.
Due Care	Shows that an organization has taken responsibility for the activities that take place within the organization and has taken the necessary steps to help protect the SOM, its resources and employees from possible risk.
Due Diligence	Is the practice by implementing controls and safeguards that make sure that the protection mechanisms are continually maintained and operational.
Information Technology Resources	Computers, storage peripherals, network equipment and wiring, network-attached printers and fax machines.
Integrity	Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose.
Trusted Partner	Is a person (i.e. vendor, contractor, 3rd party, etc.) or entity that has contracted with the State of Michigan to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

- **Authority**

  This policy obtains its authority from “1305.00 Enterprise Information Technology Policy”.

- **Enforcement**

  All enforcement for this policy shall be in compliance with 1305.00 Enterprise Information Technology Policy.

- **Developing Standards and Procedures for this Policy**

  All requirements for developing standards and procedures for this policy shall be in compliance with the Enterprise 1305.00 Information Technology Policy.

- **Exceptions**

  All exception requests to this policy must be processed in compliance with 1305.00 Enterprise Information Technology Policy.

- **Effective Date**

  This policy will be effective immediately upon release.

* * *